

FortiGate – GUIDE

Staggen und Switch aufbrechen



FortiGate Staggen

Inhaltsverzeichnis

FORTIGATE STAGGEN	3
VORWORT:.....	3
AUFBAU:	3
FORTIGATE ÜBER TFTP STAGGEN:	4
AUF DER FORTIGATE DEN INTERNAL SWITCH AUFBRECHEN	7

FortiGate Staggen

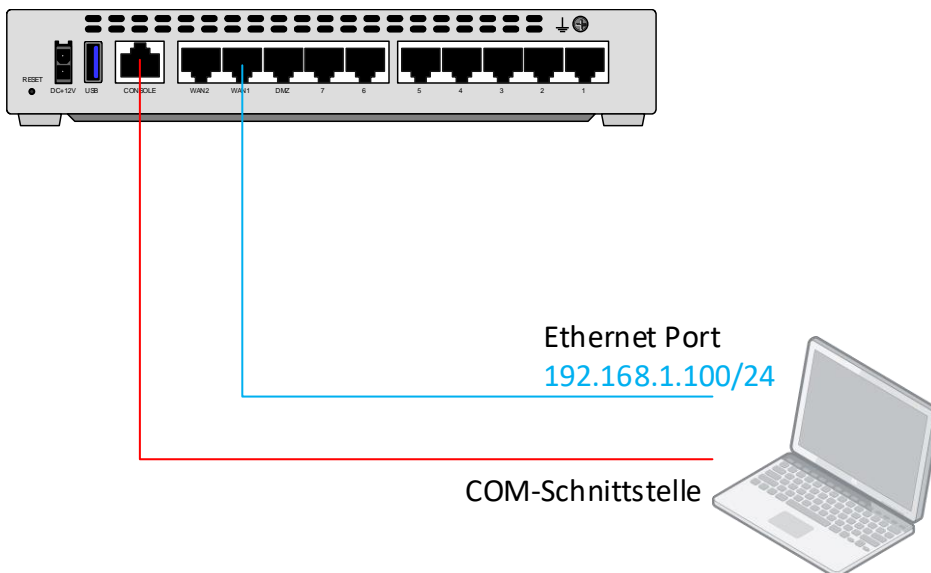
Vorwort:

In diesem Guide wird beschrieben, wie auf eine FortiGate eine x-beliebige FortiOS Version eingespielt werden kann, ohne dass der Upgrade Pfad eingehalten werden muss. Mit dieser Methode wird die ganze Konfiguration auf der FortiGate gelöscht. Die Methode eignet sich sehr gut, für eine initiale Konfiguration mit der gewünschten FortiOS Version.

Im zweiten Teil des Guides wird erklärt wie der interne Switch komplett aufgehoben werden kann und so die Interfaces separat genutzt werden können.

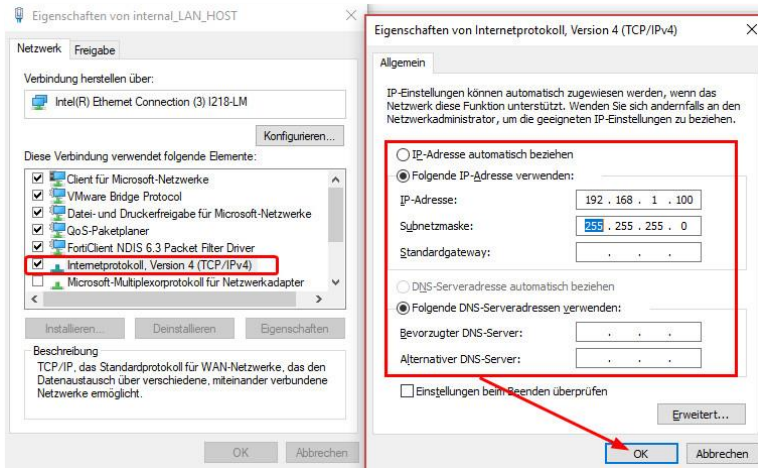
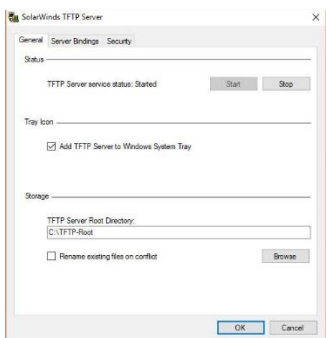
Im Guide wird von einer FortiGate 60E ausgegangen, es funktioniert aber prinzipiell mit jedem FortiGate Produkt gleich.

Aufbau:

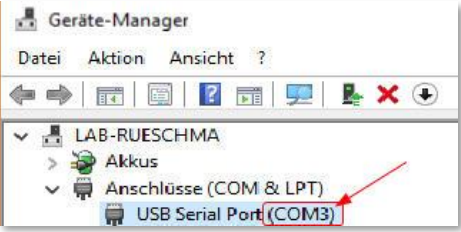


FortiGate Staggen

FortiGate über TFTP staggen:

#	Beschreibung
1	Deaktiviere sämtliche Endpoint ,Antiviren und Software Firewalls auf deinem Client aus. FortiClients oder ähnliche remote VPN Clients sind auch zu deaktivieren.
2	<p>Konfiguriere deine Netzwerkkarte mit folgender IP Adresse:</p> <p>IP Adresse: 192.168.1.100 Netzmaske: 255.255.255.0 Gateway: kein Gateway DNS: kein DNS</p> 
3	<p>Installiere einen TFTP Server. Zum Beispiel: Solarwinds</p> <p>https://www.solarwinds.com/de/free-tools/free-tftp-server</p>
4	<p>Starte das installierte TFTP Programm und starte den TFTP-Dienst.</p>  <p>Im Solarwins wird beim erstmaligen starten in deinem Root Verzeichnis ein Verzeichnis TFTP-Root angelegt.</p>
5	Kopiere das FortiOS Image in das neu angelegte Verzeichnis (meistens C:\TFTP-Root). Jetzt musst du das File folgendermassen umbenennen: image.out (achte darauf, dass du die Erweiterung out nicht nachher zweimal vorhanden hast -> image.out.out)

FortiGate Staggen

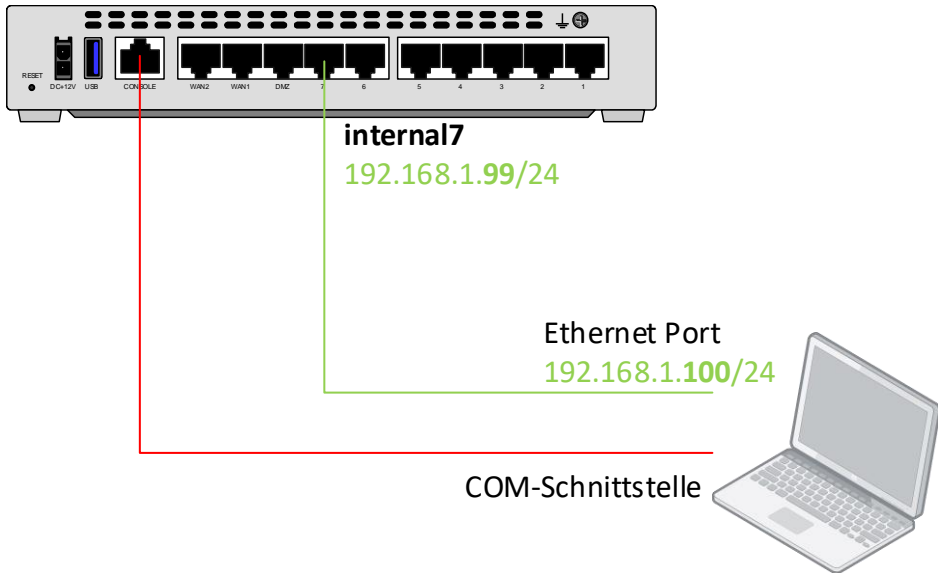
6	<p>Verbinde dich mit dem putty.exe auf die FortiGate über die COM Schnittstelle. Wenn du einen USB-Adapter benutzt, kannst du den entsprechenden COM Port im Gerätemanager nachschauen.</p> 
7	<p>Logge dich auf FortiGate ein: Benutzername: admin Passwort: <kein Passwort></p>
8	<p>Verbinde das WAN1 Interface der FortiGate mit deinem Netzwerkanschluss auf deinem Laptop.</p>
9	<p>Starte die FortiGate neu. Bitte wenn möglich nicht den Stromstecker ausziehen. Du kannst die FortiGate mit folgendem Kommando neu starten: <code>execute reboot</code></p> <pre>execute reboot</pre> <p>This operation will reboot the system! Do you want to continue? (y /n)</p> <p>Bestätige mit y</p>
10	<p>Unterbrich den Bootvorgang mit einer beliebigen Taste. Damit kommst du in das BIOS Menu der Fortigate. Du musst relativ schnell sein.</p> <pre>FortiGate-60E (16:57-06.07.2016) Ver:05000009 Serial number: FGT60E4XXXXXXX CPU: 1000MHz Total RAM: 2 GB Initializing boot device... Initializing MAC... nplite#0 Please wait for OS to boot, or press any key to display configuration menu...</pre>
11	<p>Formatiere die Firewall neu indem du die Taste F drückst. Mit yes wird das formatieren bestätigt. (yes muss ausgeschrieben werden)</p> <pre>[C]: Configure TFTP parameters. [R]: Review TFTP parameters. [T]: Initiate TFTP firmware transfer. [F]: Format boot device. [I]: System information. [B]: Boot with backup firmware and set as default. [Q]: Quit menu and continue to boot. [H]: Display this list of options.</pre> <p>Enter C,R,T,F,I,B,Q,or H: F</p> <p>It will erase data in boot device. Continue? [yes/no]: yes</p> <p>Formatting..... Done</p>

FortiGate Staggen

12	<p>Mit der Taste G wird der TFTP Upload gestartet. (Der Menu Punkt G ist im Menu nicht ersichtlich)</p> <pre>[C]: Configure TFTP parameters. [R]: Review TFTP parameters. [T]: Initiate TFTP firmware transfer. [F]: Format boot device. [I]: System information. [B]: Boot with backup firmware and set as default. [Q]: Quit menu and continue to boot. [H]: Display this list of options.</pre> <p>Enter C,R,T,F,I,B,Q,or H: G</p>
13	<p>Du kannst jetzt dreimal die Taste ENTER drücken. (Dies funktioniert nur, wenn du die Netzwerk Einstellungen und das File so konfiguriert hast, wie in diesem Guide beschrieben)</p> <p>Please connect TFTP server to Ethernet port 'WAN1'.</p> <pre>Enter TFTP server address [192.168.1.100]: Enter local address [192.168.1.1]: Enter firmware image file name [image.out]: MAC: 90:6c:ac:a6:c0:14</pre> <p>Connect to tftp server 192.168.1.100 ...</p>
14	<p>Die Software wird hochgeladen. Sobald der Upload komplett ist, wirst du gefragt, wo das Image verwendet werden soll. Wir werden es in die default Partition kopieren lassen (Taste D)</p> <pre>##### Image Received. Checking image... OK Uncompressed size: 268435968 = 0x10000200 Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]?D</pre>
15	<p>Mit der Taste y bestätigen.</p> <pre>Programming the boot device now. The system must re-layout the boot device to install this firmware. The default and backup firmware will be lost. Continue:[y/N]? .. Bootting OS... Reading boot image... 2622694 bytes. Initializing firewall..</pre>

Auf der FortiGate den internal Switch aufbrechen

#	Beschreibung/ Aufgaben
1	<p>Nachdem die FortiGate neu gestartet hat, kannst du dich folgendermassen auf das Gerät einloggen:</p> <pre>FGT60Exxxxxxx logging: admin Password: <kein Passwort eingeben> Welcome ! FGT60Exxxxxxx #</pre>
2	<p>Damit der Switch auf der FortiGate aufgehoben werden kann, müssen alle Referenzen welche mit dem Switch (internal) verbunden sind, aufgehoben werden. Bei einer initialen Konfiguration geht dies am schnellsten, indem man Policies und DHCP Server vom internal Interface löscht:</p> <p>Löschen der Policies:</p> <pre># config firewall policy # show</pre> <p>Du siehst jetzt die konfigurierten Policies</p> <pre>(policy) # purge</pre> <p>Achtung der <code>purge</code> Befehl löscht unwiderruflich alles in diesem Container. In diesem Fall alle Regeln</p> <pre>(policy) # show</pre> <p>Jetzt solltest du keine Policies mehr sehen</p> <pre>(policy) # end</pre>
3	<p>Wir löschen den DHCP Server welcher default mässig auf dem INTERNAL Interface konfiguriert ist:</p> <pre># config system dhcp server (server) # show</pre> <p>Du siehst den konfigurierten DHCP Server</p> <pre>(server) # purge</pre> <p>Der ganze Container wird gelöscht</p> <pre>(server) # show</pre> <p>Du solltest jetzt keinen DHCP Server mehr sehen</p> <pre>(server) # end</pre>
4	<p>Wir lösen den Switch INTERNAL auf:</p> <pre># config system virtual-switch (virtual-switch) # show</pre> <p>Du siehst den Switch mit allen zugewiesenen Ports.</p> <pre>(virtual-switch) # purge</pre> <p>Der ganze Virtual-Switch wird gelöscht. Dies dauert eine bis zwei Sekunden.</p> <pre>(virtual-switch) # show</pre> <p>Der Switch ist nicht mehr vorhanden</p> <pre>(virtual-switch) # end</pre>

5	<p>Wir konfigurieren das Admin Interface damit wir über GUI auf die FortiGate zugreifen können:</p> <p>Interface internal7 mit der IP Adresse 192.168.1.99/24</p> <pre># config system interface (interface) # edit internal7 (internal7) # set ip 192.168.1.99/24 (internal7) # set allowaccess https ssh ping (internal7) # end</pre> <p>Auf allen Fortinet Geräten ist die Administrations Adresse defaultmässig 192.168.1.99 konfiguriert.</p>
6	<p>Jetzt kannst du dich über das Interface 7 über den Webbrowser auf die FortiGate folgendermassen einloggen: https://192.168.1.99</p> <p>Du wirst dein LAN Kabel auf der FortiGate auf internal7 einstecken müssen.</p>  <p>internal7 192.168.1.99/24</p> <p>Ethernet Port 192.168.1.100/24</p> <p>COM-Schnittstelle</p>
7	<p>Jetzt kannst du auf deinem Client alle Antiviren, Firewalls usw. wieder einschalten.</p>